UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

CRIMINAL ACTION NO. 04-10217-GAO

UNITED STATES OF AMERICA

v.

DARREN F. WILDER,
Defendant

PROTECTIVE ORDER

November 30, 2005

IT IS HEREBY ORDERED:

1. The government shall provide defendant's counsel with: (1) a copy of the hard drive of the computer in the above-captioned matter, necessarily including any and all actual or alleged child pornography and/or contraband contained thereon (the "retained computer evidence") and (2) a copy of all of the Encase evidence files relating to this case, which includes evidence files for all media seized from defendant's work computer, necessarily including any and all actual or alleged child pornography and/or contraband contained therein (the "Encase evidence files").

2. Defense counsel shall maintain copies of the retained computer evidence as follows:

   a. Copies of the retained computer evidence shall be maintained by defense counsel in accordance with this Order, and shall be used by counsel and identified employees of his office solely and exclusively in connection with this case (including trial preparation, trial and appeal).

   b. Copies of the retained computer evidence shall be maintained by defense counsel in a locked file or cabinet at all times, except while being actively utilized as provided for in this Order.

   c. A copy of this Order shall be kept with the copies of the retained computer evidence at all times.

d. Copies of the retained computer evidence shall be accessed and viewed only by defense counsel, identified employees of defense counsel's office, and the expert retained by defense counsel in this case. Identified employees of defense counsel's office may only view the evidence in the presence of defense counsel, and only after reviewing this Order and agreeing in writing to be bound by it. Defense counsel shall maintain a list of all identified employees of his office granted access to the retained computer evidence, which list shall include the dates and times of such access.

e. Defendant himself shall not be permitted to access or view any graphic image file containing alleged child pornography or contraband on the retained computer evidence or in the Encase evidence files without petition to and prior order of this Court. However, defendant may, in the presence of defense counsel and under his direct supervision and control, access and view non-image data contained in the retained computer evidence or Encase evidence files for the purpose of assisting in the preparation of his defense.

f. Any computer into which copies of the retained evidence may be inserted for access and operation shall not be connected to any network while a copy of the retained evidence is inserted in it.

g. Any computer into which copies of the retained computer evidence is inserted may be connected to a printer only under the following conditions: (1) that any printer utilized is solely a local printer; (2) that the printer may be connected only when and as necessary to print non-graphic image files; and (3) that defense counsel and/or the defense expert hired in connection with this case shall be personally present at all times the printer is connected.

h. In no event shall any graphic image containing actual or alleged child pornography be copied, duplicated or replicated, in whole or in part, including duplication onto any external media. Defense counsel shall take the necessary steps to ensure that any alleged child pornography is not copied or saved onto any computer media or hard drive, including into unallocated space and virtual memory, except to the extent that duplication into Random Access Memory (RAM) or onto a hard drive is required by or necessarily results from the analysis conducted in connection with this case. If any alleged child pornography is copied onto the hard drive of any computer, that hard drive must be used exclusively by defense counsel or the defense expert hired in connection with this case and only for the purposes of this case until such hard drive is reformatted or otherwise wiped clean to ensure that all child pornography is removed.

3. The defense expert hired in connection with this case shall maintain and secure the Encase evidence files in the following manner:

a. Copies of the Encase evidence files shall be maintained by the defense expert in accordance with this Order, and shall be used by the defense expert solely and exclusively in connection with this case (including trial preparation, trial and appeal).

b. Copies of the Encase evidence files shall be maintained by the defense expert in a locked file or cabinet at all times, except while being actively utilized as provided for in this Order.

c. A copy of this Order shall be kept with the copies of the Encase evidence files at all times.

d. Copies of the Encase evidence files shall be accessed and viewed only by the defense expert and identified employees of the defense expert's office. Identified employees of the defense expert's office may only view the evidence in the presence of the defense expert, and only after reviewing this Order and agreeing in writing to be bound by it. The defense expert shall maintain a list of all identified employees of his office granted access to the Encase evidence files, which list shall include the dates and times of such access.

e. Any computer into which copies of the Encase evidence files may be inserted for access and operation shall not be connected to any network while a copy of any Encase evidence file is inserted in it.

f. Any computer into which copies of the Encase evidence files are inserted may be connected to a printer only under the following conditions: (1) that any printer utilized is solely a local printer; (2) that the printer may be connected only when and as necessary to print non-graphic image files; and (3) that the defense expert or an identified employee of the defense expert's office who is bound by this Order shall be personally present at all times the printer is connected.

g. In no event shall any graphic image containing actual or alleged child pornography be copied, duplicated or replicated, in whole or in part, including duplication onto any external media. The defense expert shall take the necessary steps to ensure that any alleged child pornography is not copied or saved onto any computer media or hard drive, including into unallocated space and virtual memory, except to the extent that duplication into Random Access Memory (RAM) or onto a hard drive is required by or necessarily results from the analysis conducted in connection with this case. If any alleged child pornography is copied onto the hard drive of any computer, that hard drive must be used exclusively by the defense expert hired in connection with this case and only for

the purposes of this case until such hard drive is reformatted or otherwise wiped clean to ensure that all child pornography is removed.

4. Within 30 days of termination of this case (including the termination of any appeal), defense counsel shall return (or cause the return of) all copies of the retained computer evidence and the Encase evidence files to a representative of the Federal Bureau of Investigation. Upon the return of the retained computer evidence and the Encase evidence files, defense counsel shall file a brief report to the Court specifying that the terms of this Order have been complied with and reporting the return of the copies of evidence.

IT IS SO ORDERED.

November 30, 2005
DATE

DISTRICT JUDGE